

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS**

MALIBU MEDIA, LLC,)	
)	
Plaintiff,)	Civil Action Case No. 5:19-cv-00834-DAE
)	
v.)	
)	
JOHN DOE infringer using)	
IP address 70.121.72.191,)	
)	
Defendant.)	
_____)	

**APPENDIX TO PLAINTIFF’S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR
TO A RULE 26(f) CONFERENCE AND ITS ACCOMPANYING MEMORANDUM OF
POINTS AND AUTHORITIES**

Pursuant to Rule CV-7, Malibu Media, LLC, in support of its Motion for Leave and its accompanying Memorandum of Points and Authorities, submits the following declarations:

Exhibit A: Declaration of Colette Pelissier	2
Exhibit B: Declaration of Patrick Paige	9
Exhibit C: Declaration of Tobias Fieser	20

Respectfully submitted,

By: /s/ Paul S. Beik
Paul S. Beik
Texas Bar No. 24054444
BEIK LAW FIRM, PLLC
8100 Washington Ave., Suite 1000
Houston, TX 77007
T: 713-869-6975
F: 713-868-2262
E-mail: paul@beiklaw.com
ATTORNEY FOR PLAINTIFF

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS**

MALIBU MEDIA, LLC,)	
)	
Plaintiff,)	Civil Action Case No. 5:19-cv-00834-
DAE)	
)	
v.)	
)	
JOHN DOE infringer using)	
IP address 70.121.72.191,)	
)	
Defendant.)	
_____)	

**DECLARATION OF COLETTE PELISSIER IN SUPPORT OF PLAINTIFF’S MOTION
FOR LEAVE TO TAKE DISCOVERY PRIOR TO A RULE 26(f) CONFERENCE**

[Remainder of page intentionally left blank]

**DECLARATION OF COLETTE PELISSIER IN SUPPORT OF
PLAINTIFF'S MOTION FOR LEAVE TO SERVE A THIRD PARTY
SUBPOENA PRIOR TO A RULE 26(f) CONFERENCE**

I, COLETTE PELISSIER, DO HEREBY DECLARE:

1. I am over the age of eighteen (18) and otherwise competent to make this declaration.

2. The facts stated in this declaration are based upon my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

3. I own Malibu Media d/b/a as X-Art.com. No other person or entity has or can claim an ownership interest in the X-Art.com movie copyrights.

4. I developed the X-Art.com business plan in 2010 while still working full time as a realtor in the Los Angeles market. X-Art.com was created to address the lack of artistically produced adult oriented content suitable for upscale women and couples.

5. I invested significant time, along with all of my available financial resources, into the production of content for the new X-Art.com website. I knew that the adult content industry was in financial crisis, and the odds of success for a new adult website were low.



6. After a difficult start, and with much effort, I was able to perfect the X-Art genre thus propelling the X-Art.com website into one of the top websites of its kind worldwide.

7. X-Art.com customers can pay a monthly recurring subscription fee of \$29.95, or an annual subscription fee of \$99.95 to access our entire library of HD Video content.

8. Internet subscription sales are and have always been by far X-Art.com's primary source of revenue, however, recent additional revenue streams have been created through the licensing of X-Art content to Fortune 500 companies operating within the hospitality industry.

9. As X-Art's subscriber base has grown, our production expenditures have also grown. We spend over two million dollars a year producing content, and millions more each year to run our business.

10. For the first several years of operation, X-Art did not have significant issues with piracy. However, once our content became well known and highly desirable, X-Art movies started ranking as the most downloaded adult content on several of the most popular torrent websites.

11. Currently we have tens of thousands of paying subscribers, but we are finding it hard to grow and maintain our subscriber base as so many of our movies are distributed for free, without authorization, by users of the Bittorrent

Network. X-Art must protect its copyrights in order to survive and for any hope for future revenue growth.

12.The only redress against Bittorrent based piracy is to initiate lawsuits against the Bittorrent users responsible for these unauthorized distributions.

13.These lawsuits must be filed as "John Doe" lawsuits because the identity of the infringer is initially unknown to us. From my experience filing similar cases against other defendants throughout the country, once provided with the IP Address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address and phone number of the applicable subscriber in control of that IP address at the stipulated date and time.

14.The proper forum for these lawsuits is determined by using Maxmind Premium Geolocation services. Founded in 2002, Maxmind's website cites it as an industry-leading provider of geolocation databases¹. It is also used by state and federal law enforcement in the prosecution of computer and cybercrimes.

15.Since January 2013, Malibu Media has used this geolocation procedure to determine the proper District for filing in 5,349 cases. Out of these 5,349 total cases, 5,334 have accurately traced to the District Court in which the case was filed. This translates to a 99.99% chance of proper personal jurisdiction and venue pursuant to the Maxmind Geolocation trace.

¹ www.maxmind.com



16. Over the past several years, Malibu Media has employed two experts to track and scan the infringement of its movies - Excipio GmbH ("Excipio") and IPP International U.G. ("IPP").

17. Investigators from both companies have testified in court and have attested to the reliability of the applicable forensic technology. Malibu Media has also independently tested each system to ensure the highest level of accuracy.

18. Each recorded infringement enumerated on Exhibit A to the Complaint in this lawsuit was documented by either IPP or Excipio. In many instances, infringing transactions were documented by both entities. Each Single Movie Hash on Exhibit A was fully downloaded and compared side by side to a control copy supplied to the applicable investigator by Malibu Media.

19. Malibu Media's intention in bringing these lawsuits is not to cause financial hardship but instead to deter infringement and be compensated for the intentional theft of its videos.

20. I have consistently instructed all attorneys representing Malibu Media in these lawsuits to seek and be open to exculpatory evidence and to be cautiously prudent when pursuing these claims. We do not pursue our claims against all Doe Defendants. For example, once receiving discovery, we may learn that a Defendant is on active duty in the military and we will dismiss that case. Also, we may learn a Defendant is possibly a coffee shop with open wireless, or some other circumstance that would prevent us from pursuing our claims. When

discovery indicates that pursuing the case will present for undue hardship for the Defendant, my instructions to my lawyers are to dismiss the case.

21. We invest significant resources into pursuing all types of anti-piracy enforcement, such as Digital Millennium Copyright Act ("DMCA") takedown notices and direct efforts aimed at infringing websites. We are even working with law enforcement to stop the piracy of our movies.

22. Despite sending thousands of DMCA notices per week, the infringement continues. And, if one searches for "X-Art" on a torrent website, the site will reveal thousands of unauthorized torrents available for free.

23. I have never authorized anyone to put our works on a torrent website.

24. I firmly believe that we must exercise our rights under the Copyright Act to prevent infringement. Otherwise, we face an immediate and serious risk. It is simply impossible to compete with free.

25. We do not seek to use the Court system to profit from the infringement like some have suggested. As previously stated, revenues from subscriptions to X-Art.com are by far and away the dominant driver of Malibu Media's business. We want the infringement to stop. The purpose of these lawsuits is to motivate people to pay for subscriptions by deterring infringement and seek some reasonable compensation for the massive amount of infringement of our copyrights.



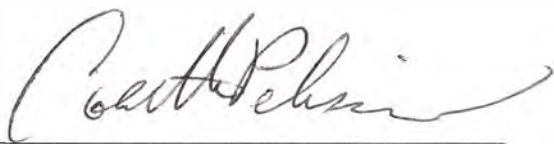
26.It is my hope that by upholding the law, the courts will protect our ability to continue with our dream and allow all creative people the ability to make a living by distributing their work in this fast-paced digital age.

27.In conclusion, we want the courts to know that we are a small business and we need the law to be enforced to ensure our survival. It is getting more difficult for us every day and we hope that in the future there will be a better way to protect our copyrights.

28.Thank you in advance for your time and consideration of this matter, please do not hesitate to ask if we can clarify any further questions.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

By: 

COLETTE PELISSIER

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS**

MALIBU MEDIA, LLC,)	
)	
Plaintiff,)	Civil Action Case No. 5:19-cv-00834-
DAE)	
)	
v.)	
)	
JOHN DOE infringer using)	
IP address 70.121.72.191,)	
)	
Defendant.)	
_____)	

**DECLARATION OF PATRICK PAIGE IN SUPPORT OF PLAINTIFF’S MOTION FOR
LEAVE TO TAKE DISCOVERY PRIOR TO A RULE 26(f) CONFERENCE**

[Remainder of page intentionally left blank]



Computer Forensics, LLC
1880 N. Congress Ave Suite 333
Boynton Beach, FL 33426
Main: 561.404.3074
www.ComputerForensicsLLC.com

**EXPERT REPORT REGARDING TESTING OF IPP INTERNATIONAL UG'S
INFRINGEMENT DETECTION SYSTEM**

Prepared By: Patrick Paige, EnCE SCERS
Managing Member
Computer Forensics, LLC

DECLARATION OF PATRICK PAIGE

I, PATRICK PAIGE, DO HEREBY DECLARE:

1. I am over the age of eighteen (18) and otherwise competent to make this declaration. The facts stated in this declaration are based upon my personal knowledge.

2. I was a police officer from 1989 until 2011 for the Palm Beach County Sheriff's Office. And, from 2000-2011, I was a detective in the Computer Crimes Unit. After leaving the Palm Beach County Sheriff's Office, I founded Computer Forensics, LLC, where I am currently employed.

3. I have taken over 400 hours of courses designed to teach people how to conduct computer forensic examinations.

4. Also, while working from 2003-2011 for Guidance Software, the makers of EnCase, I taught over 375 hours of courses in computer forensics ranging from beginner to advanced levels.

5. As a computer crimes detective for the Palm Beach County Sheriff's Office, I have conducted forensic computer examinations for:

- (a) Broward County Sheriff's Office (BSO);
- (b) Federal Bureau of Investigation (FBI);
- (c) U.S. Customs and Border Protection (CBP);
- (d) Florida Department of Law Enforcement (FDLE);
- (e) U.S. Secret Service;
- (f) Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and
- (g) Various municipalities in the jurisdiction of Palm Beach County.

6. I have had students in my courses from various government branches, including: (a) sheriff's offices; (b) FBI agents; (c) ATF agents; (d) agents from the Central Intelligence Agency; and (e) individuals from other branches of government and the private sector.

7. I have received the following awards and commendations:

- (a) 1991 – Deputy of the Year, awarded by the 100 Men's Club of Boca Raton & Rotary Club.
- (b) 1997 – Deputy of the Month for June.
- (c) 2001 – Detective of the Month for October.
- (d) 2002 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jerrold Levy* case.
- (e) 2003 – U.S. Customs Service Unit Commendation Citation Award for computer forensic work in Operation Hamlet. Operation Hamlet was one of the largest rings in the history of U.S. Customs of individuals who were molesting their own children, and transmitting the images and video via the Internet.
- (f) 2005 – Detective of the Month for December.
- (g) 2006 – Letter of Commendation issued by the FBI for outstanding computer forensic work in the *U.S. vs. Frank Grasso* case.
- (h) 2007 – Outstanding Law Enforcement Officer of the Year, awarded by the United States Justice Department for work in the *U.S. vs. Jimmy Oliver* case.

8. I have testified as a fact and expert witness on numerous occasions in the field of computer forensics in both trial-level and appellate proceedings before state, federal, and military courts in California, Florida, Indiana, New Jersey, New York, and Pennsylvania.

9. No court has ever refused to accept my testimony on the basis that I was not an expert in computer forensics. My skill set and my reputation are my most important assets in my current position with Computer Forensics, LLC.

10. As part of my duties within the Computer Crimes Unit at the Palm Beach County Sheriff's Office, I investigated cases involving the use of the Internet, including cases involving peer-to-peer file sharing networks. In this role, I also investigated Internet child pornography and computer crime cases.

11. I was assigned to the Computer Crimes Unit that worked in conjunction with a private company called TLO Corp.

12. When I worked with TLO Corp., I supervised the other detectives assigned to the unit, which consisted of six online investigators and two computer forensic examiners.

13. In my experience, during the initial phase of Internet based investigations, the offender is only known to law enforcement by an IP address.

14. The only entity able to correlate an IP address to a specific individual at a given date and time is the Internet Service Provider ("ISP").

15. Once provided with the IP Address, plus the date and time of the detected and documented activity, ISP's can use their subscriber logs to identify the name, address, email address and phone number of the applicable subscriber in control of that IP address at the stipulated date and time.

16. With regard to my experience investigating child pornography cases, I supervised police officers whose responsibility it was to establish a successful TCP/IP connection with persons who were sending pornographic images of children or other illegal content over the Internet using peer-to-peer file sharing programs.

17. The offenders' IP addresses, as well as the dates and times of the illegal transmission were recorded.

18. An officer would then request that the assistant state attorney subpoena the corresponding ISPs for the purpose of identifying the subscribers that were transmitting the illegal content.

19. In these cases, the subscribers were not notified by the ISPs that their identity was being subpoenaed because they could have deleted the images and destroyed the data.

20. After receiving the subscribers' identities, we would prepare a search warrant that would authorize us to enter the subscribers' dwelling and seize all of their computer devices.

21. I was directly involved in approximately 200 search warrants either by way of managing the process or performing it personally while at the Computer Crimes Unit.

22. From my experience, Plaintiff is likely to identify the infringer. Indeed, during my time in the Computer Crimes Unit, I can recall only one instance in all the times that we executed a search warrant and seized computers, where we did not find the alleged illegal activity at the dwelling identified in the search warrant.

23. In that one instance, the Wi-Fi connection was not password protected, and the offender was a neighbor behind the residence.

24. I never came across a Wi-Fi hacker situation.

25. In my opinion, a child pornographer has a greater incentive to hack someone's Wi-Fi connection than a BitTorrent user because transmission of child pornography is a very serious crime with heavy criminal penalties, and many offenders can face life sentences if convicted.

26. The process used by law enforcement mirrors the process used by Malibu Media and IPP to correlate an IP address to an individual.

27. In order to ascertain the identity of the infringer, just as with law enforcement, Malibu Media must subpoena the ISP to learn the subscriber's true identity.

28. I tested IPP International U.G.'s ("IPP") infringement detection system. The infringement detection system is named "Observer." It is owned and used by IPP to identify individuals who are illegally downloading and distributing content via BitTorrent. This technology and similar investigative methods are used by law enforcement officials when tracking individuals who transmit contraband files such as child pornography via the Internet.

29. I tested IPP's infringement detection system for its accuracy in detecting and recording infringement via BitTorrent, ascertaining an infringing IP address¹, and identifying the "test" files being distributed on BitTorrent.

30. To conduct this test, I first downloaded four public domain movies from the national archive.

31. I then encoded text into each video. The purpose of this encoding was to ensure that when the file is located and download by IPP, it could be easily identified as the videos I personally encoded and seeded.

32. I then setup and configured four computers, each of which was connected to the Internet and each computer was configured with its own unique static IP address.

33. I then configured three computers with a Windows 7 operating system, and the fourth computer was a MacBook Pro configured with OS X El Capitan version 10.11.4. I installed a different BitTorrent client² onto each computer system as listed below:

¹ An IP address is a numerical value assigned to a computer or device that transmits and receives data via the Internet. When a computer user accesses the Internet, their Internet Service Provider assigns them a unique IP address for that session. In order to identify a computer user who is downloading files via the Internet, one must be able to identify the IP address the user was using at that exact time and date of downloading.

² A BitTorrent client is software that enables the BitTorrent protocol to work.

<u>Computer</u>	<u>Operating System</u>	<u>BitTorrent Client</u>
Dell Laptop	Windows 7	uTorrent Version 3.4.7
Dell Laptop	Windows 7	qBittorrent Version 3.3.4
Dell Laptop	Windows 7	Transmission Version 2.84
MacBook Pro Laptop	OS X El Capitan 10.11.4	uTorrent Version 1.8.7

34. After installing the BitTorrent clients, I also installed Wireshark and WinDump onto each computer. Wireshark and WinDump are programs that capture network traffic and create PCAP files. PCAP stands for “packet capture.” PCAPs are akin to videotapes. Indeed, a PCAP is like a video recording of all the incoming and outgoing transactions of a computer. I have used Wireshark and WinDump software while in law enforcement to examine network traffic while investigating P2P cases.

35. After installing Wireshark and WinDump onto each of the computers, I transferred the movie files that I created for the test to each of the four computers.

36. I then used one of the BitTorrent clients on the test computers to make .torrent files. I then seeded the four test movies.

37. On June 3, 2016 the test was conducted. Given only the torrent files, IPP was able to correctly identify all four static IP addresses for each of the test computers that were seeding the movies within minutes of starting the test. Soon after the test, IPP sent me the PCAP files they recorded during the test for each one of my static IP addresses.

38. I reviewed IPP’s PCAPs vis-à-vis the PCAP log files created by each of my test computers, and determined that IPP’s PCAPs match my PCAPs. This could not have happened unless IPP’s server was connected to the test computers because the transactions would not match.

39. I also conducted an examination of IPP’s PCAPs to determine if the detection software can accurately identify the BitTorrent clients I used during the test. Using Wireshark

software I loaded IPP's PCAPs recorded on the day of the test. IPP's system was able to accurately record the names and version numbers of all four BitTorrent client's software I used on each of the test computers.

40. When a BitTorrent client is installed onto a computer, the computer randomly selects a port number for its network communication. A port number is an integer ranging from 0 to 65535. The following is a chart listing the port number assigned to each of the test computers:

<u>Computer</u>	<u>BitTorrent Client</u>	<u>Port</u>
Dell Laptop	uTorrent Version 3.4.7	51892
Dell Laptop	qBittorrent Version 3.3.4	8999
Dell Laptop	Transmission Version 2.84	51413
MacBook Pro Laptop	uTorrent Version 1.8.7	10088

41. Examination of IPP's PCAP revealed that the port numbers recorded by IPP's system matched the port numbers from the test computers used for BitTorrent communications. Accordingly, my analysis confirmed that IPP was able to accurately identify the port number assigned to each test computer's BitTorrent client.

42. From this test, I concluded that IPP's infringement detection system worked, and had a subpoena been issued for my IP addresses, it would have revealed my identity. I also concluded that IPP's infringement detection system accurately identifies the BitTorrent clients as well as the BitTorrent client's port number.

43. In the past, Malibu has also retained Excipio GmbH's ("Excipio") to track infringement of Malibu's copyrighted works. In June 2013, in anticipation of the Bellwether trial in the Eastern District of Pennsylvania, I conducted a test of Excipio's infringement detection system. After performing the test, I concluded that Excipio's infringement detection system works. Specifically, the system accurately records the IP address of a person using

BitTorrent to transmit data to Excipio's computer servers. Excipio's system operates nearly the same fashion as IPP's system.

44. In addition to testing Malibu's investigators' systems, I have also conducted computer forensic examinations for Malibu in their copyright infringement cases throughout the country.

45. Indeed, in my role as an expert for Plaintiff, I have examined countless computer hard drives for evidence of: (a) the use of BitTorrent; (b) infringement of the copyrighted "X-Art" works owned by Plaintiff; (c) spoliation of evidence; and (d) suppression of evidence. These examinations have revealed either: (1) evidence of copyright infringement of Malibu Media, LLC's works; or (2) evidence of suppression and spoliation. Sometimes I have found both. By way of illustration, below are examples where Malibu obtained a Defendant's hard drive and discovered evidence of its movies, spoliation, and/or defendants' failures to disclose all hard drives.

- a. *Malibu Media, LLC v. Weaver*, No. 8:14-cv-01580-VMC-TBM (M.D. Fla. 2015): In *Weaver*, the Court ordered production of the hard drives, and my forensic examination revealed evidence which irrefutably demonstrated: (a) Defendant's BitTorrent use; (b) the prior existence of numerous X-Art titles; (c) the deletion of BitTorrent files and uninstallation of a BitTorrent client; and (d) the existence of other computer devices that have not been produced. Because of this examination, Malibu was able to successfully disprove Defendant's denial of infringement.
- b. *Malibu Media, LLC v. Huseman*, No. 1:13-cv-02695-WYD-MEH (D. Colo. 2014): In the *Huseman* case, I discovered evidence of: (a) BitTorrent use; (b) the prior existence of numerous X-Art titles; (c) the deletion of BitTorrent files and uninstallation of a BitTorrent client; and (d) the existence of other computer devices that had not been produced to me for examination, one of which contained titles of Plaintiff's copyrighted works. Ultimately, the parties stipulated to a final judgment in favor of Malibu Media, LLC.
- c. *Malibu Media, LLC v. John Doe*, No. 1:14-cv-10155-KBF (S.D.N.Y. 2015): My forensic examination revealed that defendant had over eleven different file destruction software programs on his hard drive – each with the capability of destroying substantial amounts of data. He used several of the software programs

just days before turning it over for imaging and examination. I also detected that prior to defendant's use of the file destruction software, the defendant connected another undisclosed external storage device to his hard drive. This suggested that defendant was storing data which he wanted to retain prior to using the file destruction software programs on his hard drive. Ultimately, the defendant admitted to his infringement and apologized to Malibu.

- d. *Malibu Media, LLC v. Tashiro*, No. 1:13-cv-00205-WTL-MJD (S.D. Ind. 2014): My examination revealed that defendants deleted thousands of BitTorrent files the night before producing the hard drives for imaging. My examination also revealed that defendants possessed and used other hard drives which were never disclosed or produced during discovery. Ultimately, the court imposed terminating sanctions against defendants for failure to disclose documents, spoliation, and perjury.
- e. *Malibu Media, LLC v. John Doe*, No. 12-2078 (E.D. Pa. 2013): In this "Bellwether" case, my examination of defendant's hard drive revealed that he installed a Windows operating system three (3) days after being served with a subpoena for production of his computer device. This installation resulted in the complete destruction of all files contained within the hard drive prior to the Windows installation. After falsely testifying, Defendant admitted that he had downloaded Plaintiff's copyrighted works and had wiped his desktop computer (by installing a new Windows operating system) to conceal the infringements. In the end, the Court entered a substantial judgment in favor of Malibu.

46. I am paid on an hourly basis by Malibu Media, LLC, at the rate of \$325.00 per hour for pre-trial investigative work, although the fee increases if I am required to testify at trial.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 19th day of August, 2016.

By: _____

PATRICK PAIGE

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS**

MALIBU MEDIA, LLC,)	
)	
Plaintiff,)	Civil Action Case No. 5:19-cv-00834-
DAE)	
)	
v.)	
)	
JOHN DOE infringer using)	
IP address 70.121.72.191,)	
)	
Defendant.)	
_____)	

**DECLARATION OF TOBIAS FIESER IN SUPPORT OF PLAINTIFF’S MOTION FOR
LEAVE TO TAKE DISCOVERY PRIOR TO A RULE 26(f) CONFERENCE**

[Remainder of page intentionally left blank]

**DECLARATION OF TOBIAS FIESER IN SUPPORT OF PLAINTIFF'S MOTION FOR
LEAVE TO TAKE DISCOVERY PRIOR TO A RULE 26(f) CONFERENCE**

I, TOBIAS FIESER, HEREBY DECLARE:

1. My name is Tobias Fieser.
2. I am over the age of 18 and am otherwise competent to make this declaration.
3. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.
4. I am employed by IPP International UG ("IPP"), a company organized and existing under the laws of Germany, in its litigation support department.
5. Among other things, IPP is in the business of providing forensic investigation services to copyright owners.
6. IPP's system has been monitoring the BitTorrent file distribution network for the presence of Malibu Media's copyrighted works since 2011. IPP's forensic software identifies Internet Protocol ("IP") addresses that are being used by infringers to distribute Malibu Media's copyrighted works within the Bittorrent File Distribution Network.
7. IPP tasked me with effectuating, analyzing, reviewing and attesting to the results of this investigation. I have previously provided the same support for Malibu Media in thousands of lawsuits across the United States, and I gave full and complete testimony about the workings of IPP's forensic scan during the "Bittorrent Bellwether Trial" (*Malibu Media v. John Does*, 12-cv-2078, (E.D. Pa.)).
8. Infringement of Malibu Media's movies occurs within two formats. The first entails distribution of a specific single movie file correlating to a copyrighted Malibu Media movie. The second involves large scale distribution utilizing "Unauthorized Packs" (commonly referred to as 'siterips').

9. Upon review of IPP's forensic activity logs, I determined that IPP's forensic servers connected to an electronic device using IP Address 70.121.72.191. Consequent to this connection, the IP Address used by Defendant of 70.121.72.191 was documented distributing to IPP's servers multiple pieces of Malibu Media's copyrighted movie titled Kaisa Slippery and Wet at exactly 5/5/2019 7:59:08 AM. This time is quoted in Universal Time which correlates to the assignment logs kept by US ISPs tracking which IP Address is assigned to which customer at a given point in time.

10. A digital file can be identified by what is called a "Cryptographic Hash Value." This concept was developed by the United States National Security Agency. IPP's software determined that the file being distributed by Defendant using the IP Address of 70.121.72.191 at 5/5/2019 7:59:08 AM has a unique identifier of the Cryptographic Hash of 1B2CFE6B8C36391FC2B1F53792A5D35DD87AF510.

11. A full copy of the digital file identified by the Hash of 1B2CFE6B8C36391FC2B1F53792A5D35DD87AF510 was downloaded by IPP's software, and I confirmed this file is a digital movie file. I further viewed this file and determined it was substantially similar to Malibu Media's copyrighted movie titled Kaisa Slippery and Wet.

12. IPP's software is unable to distribute content; it is programmed to only allow it to download files from the Bittorrent Network. At no point did IPP distribute any part of Plaintiff's copyrighted movies at any time.

13. It is theoretically possible to "spoof" an IP Address on the Internet. However, it is not possible to spoof an IP Address within the context of a TCP/IP connection. I verified that a TCP/IP connection was made between IPP's investigative servers and the electronic device using IP Address 70.121.72.191 and that multiple bits were conveyed over this connection.

Consequently, it is impossible that another party was "spoofing" the IP Address used by Defendant.

14. IPP additionally confirmed through its ancillary worldwide BitTorrent surveillance program that IP address 70.121.72.191 is associated with significant long term BitTorrent use.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 461 day of July, 2018.

TOBIAS FIESER

By: 